INFORMATION AND CONTROL 6, 315–330 (1963)

Error-Correcting Codes: An Axiomatic Approach*

E. F. ASSMUS, JR.† AND H. F. MATTSON

Applied Research Laboratory, Sylvania Electronic Systems, A Division of Sylvania Electric Products, Inc., Waltham, Massachusetts

This paper emphasizes that coordinates of an error-correcting code are functions. We have incorporated certain ideas already present in the literature into an axiomatic treatment of error-correcting codes. The usual "coordinates" are functions defined on a set of messages, with values in a given set K (classically, $K = \{0, 1\}$). These functions are required to satisfy a certain "Coding Axiom". In Section II we treat linear codes, K now being a finite ring; and we also give a treatment of cyclic codes, where we prove that the minimum distance is at least n/k, where n is the block length and k the dimension. In Section III we prove our main result, the Mapping Theorem, which relates the weights in a code A to those in an image-code B; image-codes are defined simply in our terms. A number of corollaries are noted, including a formula for the sum of the squares of the weights of all code elements.

I. CODES AND MAPS OF CODES

An error-correcting code is commonly defined as a subset of vector space over 0, 1. Our approach emphasizes the role of the coordinate functions.

On terminology there is one possible source of confusion that should be mentioned at the outset. Our "alphabet" is *not* the "alphabet" of the fundamental papers of Slepian. Instead we use the term as Wolfowitz (1957) does to mean the set of symbols used to record the "messages" or "ideas" to be transmitted. Those familiar with the subject need only think "zero-one" when seeing "alphabet."

We fix for the present an alphabet K. Our code will be defined with respect to this alphabet. We take K to be a finite set of at least two elements.

* Part of the work on this paper was performed under Contract No. AF19(604)-8516 from the Air Force Cambridge Research Laboratories.

† Wesleyan University, Middletown, Connecticut.

We define a *code* as a set A, to be called the "message set," together with an indexed collection $\{f_\alpha \mid \alpha \in \mathfrak{A}\}$ of functions from A to K, to be called the "encoding" or "coordinate" functions.[1]

The data must satisfy but one axiom:

(*Coding Axiom*) *For each pair of distinct elements a and b of the message set there is an encoding or coordinate function f such that* $f(a) \neq f(b)$.

Observe that given a set A together with a collection of functions from A to K one obtains a code by taking quotients. (Such a set and functions would, most properly, be called a *precode*.) Thus one checks easily that the following relation

$$a \equiv b \quad \text{if and only if} \quad f_\alpha(a) = f_\alpha(b) \quad \text{for all} \quad \alpha \in a$$

is an equivalence relation on the set A and that the set of equivalence classes together with the functions induced on this set by the original functions is a code.

Abusing our terminology, we will frequently denote the code simply by A, suppressing the mention of the encoding functions in the denotation.

First, let us show that our codes are subsets of direct products. Assume the set $\mathfrak{A}$ has cardinality n, called the *block length* of the code. Let V be the direct product of K with itself n times, indexed by $\mathfrak{A}$. Then we realize the code A as a subset of V by the function $F: A \to V$ given by: $F(a)$ is the vector whose αth coordinate is $f_\alpha(a)$. The coding axiom ensures that F is one-to-one. Hence, the familiar subset is merely the image of A under F. We call this image $F(A)$ the (concrete) realization of the code A.

Conversely, suppose we are given a subset A of the direct product, V, of K with itself n times. Let $\mathfrak{A}$ be the indexing of the product, and let p_α, $\alpha \in \mathfrak{A}$ be the αth projection of V on K. Then the code associated with this subset is given as follows: The message set is A, and the encoding functions are the restrictions of the p_α to A.

Given two codes A and B, a *map*, ϕ, *of* A *into* B is a set-theoretic function from A to B with the property that for each encoding function g of B, $g\phi$[2] is an encoding function of A.[3]

[1] We have restricted ourselves to encodings which use the same number of letters in each word, thus to so-called "block codes." Our definition of codes grew out of the "modular representation table" in Slepian's fundamental paper (1956).

[2] Here juxtaposition denotes the composition of functions.

[3] The mathematician familiar with homological algebra will realize that we

Examples of maps of codes are easily found. Suffice it to mention now that given a code A if we select certain of the encoding functions of A and with these construct the code attached to the precode they yield by the quotient process described above, then the natural map of A into this quotient is a map of codes. In this familiar process, called "shortening the code," the encoding functions usually selected still distinguish A (i.e., the equivalence relation is the identity relation).

We do not assume the index set $\mathfrak{A}$ ordered, and hence we do not really distinguish between codes equivalent in Slepian's sense. That is, we prefer not to think of our words as ordered. Of course one can easily do so when necessary, e.g., when discussing burst-error correction or cyclic codes.

We shall denote the number of elements in K by q and the block length by n. Then the cardinality of A is always at most q^n.

A subset $\mathfrak{A}'$ of $\mathfrak{A}$ (the indexing set for the encoding functions) will be called an *information set* provided the collection $\{f_{\alpha'}, \alpha' \in \mathfrak{A}'\}$ distinguishes A, but no proper subset of $\mathfrak{A}'$ will give distinguishing encoding functions. Thus $\mathfrak{A}'$ is an information set if the precode given by $A; f_{\alpha'}, \alpha' \in \mathfrak{A}'$ is in fact a code but no further "shortening" of A is also a code.

The *dimension* of a code A is defined here as the minimum of the cardinalities of the information sets of A.[4] Clearly, for any code A the cardinality of A is less than or equal to $q^{\dim A}$; furthermore, $\dim A \leqq n$. If there is an information set of A of cardinality k and the cardinality of A is q^k, then every information set has cardinality at least k. This is the situation of most interest, and if A is such a code, we call it an (n, k) *code*.

In the next section we shall impose some structure on both alphabet and message set and introduce the Hamming weight. (We then discuss cyclic codes in our terms, prove a new lower bound on the minimum

---

have essentially described the category of codes over K. He might like to prove the following facts about the category: (1) Finite direct products and sums exist. (2) For each cardinal number m the empty set (as message set) together with the empty function repeated m times is a code, and all such are isomorphic in the category. (3) Given a code A in which each distinct coordinate function is repeated m times we have another code A' with the same message set and coordinate functions the distinct coordinate functions of A, and if ϕ_m denotes the code of (2), A is the direct sum of A' and ϕ_m .

[4] In the familiar case where A is a finite-dimensional vector space over the field K and the encoding functions are linear functionals, the coding axiom ensures that the linear dimension of A is the same as the code-dimension.

weight in cyclic codes, and give a simple proof that linear codes over a finite field are systematic.)

II. LINEAR CODES OVER A FINITE RING

The general setting of Section I was not quite structured enough to permit detailed analysis. We therefore make the following further assumptions:

1. The alphabet is a ring.
2. The message set is a module over the alphabet.
3. Encoding functions and maps of codes are module-homomorphisms.

Under these assumptions[5] the coding axiom becomes

$$\text{Coding Axiom: } \bigcap_{\alpha \in \mathcal{A}} \operatorname{Ker} f_\alpha = 0,$$

where $\operatorname{Ker} f_\alpha$ denotes the kernel of the encoding function f_α ; i.e., the set of all $a \in A$ such that $f_\alpha(a) = 0$.

Thus, we are discussing linear codes, also called group codes, although our situation is somewhat more general since the alphabet is not necessarily a finite field.

Given a finite ring K define $\chi: K \to Z$ (the ring of rational integers) by $\chi(0) = 0$, $\chi(a) = 1$ for $a \neq 0$. (χ is merely a function with no relation to the imposed structure.)

Define the *Hamming weight*[6] of an $a \in A$ by

$$w(a) = \sum_{\alpha \in \mathcal{A}} \chi(f_\alpha(a)). \tag{1}$$

[5] We continue under the assumptions made in Section I that our alphabets and block lengths are finite. If he wishes, the reader may assume that the alphabet is a field; then, the message set becomes a finite-dimensional vector space over that field, the encoding functions become linear functionals, and maps of codes become linear transformations. (Of course a linear transformation is not a map of codes unless it satisfies the additional condition listed in Section I.)

[6] The Hamming weight is but one of a general class of weight functions possible for codes. Let E be any nonempty subset of $V = K \times \cdots \times K$, let $a \in V$, and define $w(a)$ as follows: Set $w(0) = 0$; if $a \neq 0$ has the form $a = \pm a_1 \pm \cdots \pm a_j$, with each $a_i \in E$, define $w(a)$ as the inf. of such j's; otherwise set $w(a) = \infty$. For the Hamming weight, E is simply the set of all vectors having only one nonzero coordinate. For further information, see (Prange, 1961, (1.5)).

The Hamming weight $w(a)$ is an integer satisfying $0 \leqq w(a) \leqq n$, and $w(a) = 0$ if and only if $a = 0$. It is a norm giving the usual metric; we shall denote the minimum distance in the code by d.

We will usually denote χf_α by χ_α and then (1) becomes

$$w(a) = \sum_{\alpha \in \mathfrak{A}} \chi_\alpha(a). \tag{1'}$$

The following proposition uses the assumption (satisfied automatically when K is a field) that all encoding functions are onto.[7]

PROPOSITION (after Prop. 6 of (Slepian, 1956)). Let A be an (n, k) linear code over the finite ring K. Assume that all encoding functions map A onto K. Then

$$\sum_{a \in A} w(a) = (q - 1)nq^{k-1}.$$

The proof, omitted here, is a simple counting argument. The proposition yields the familiar Plotkin bound,

$$d \leqq (q - 1)nq^{k-1}/(q^k - 1)$$

with equality if and only if all nonzero code-elements have the same weight.[8]

In the next section we will give an elaboration of this simple counting argument in proving a general theorem connecting the weights of the elements of a code and those of any homomorphic image.

Suppose $A; f_\alpha, \alpha \in \mathfrak{A}$ is a linear code over K (where each f_α is assumed to be onto). Then, for each α, we have $A/\mathrm{Ker} f_\alpha \approx K$. Now, if f_{α_1} and f_{α_2} are encoding functions with kernel f_{α_1} = kernel f_{α_2} we can replace one by the other without affecting the code or the Hamming weight. That is, the two isomorphisms

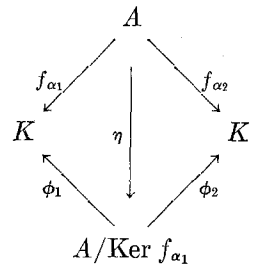
$$\phi_1 : A/\mathrm{Ker} f_{\alpha_1} \to K \quad \text{and} \quad \phi_2 : A/\mathrm{Ker} f_{\alpha_2} \to K$$

yield an automorphism $\phi = \phi_2\phi_1^{-1}$ of K viewed as K-module; we have the

[7] This assumption is reasonable in the sense that full use of a component in the realization of a code requires that every letter of the alphabet should appear.

[8] This bound appears in several places, e.g., (Bose and Kuebler, 1960, p. 124), (MacWilliams, 1961, p. 294), (McCluskey, 1959, p. 1498), (Peterson, 1961), (Weinitschke, 1957, p. i). Some of the proofs seem circuitous; the proof in Weinitschke (1957) is the simplest one.

following commutative diagram (where η is the natural map):



Thus $f_{\alpha_2} = \phi f_{\alpha_1}$; and ϕ together with the identities on the other coordinates yields an automorphism of $K \times K \times \cdots \times K$; it takes the realization of A onto an isomorphic submodule of $K \times K \times \cdots \times K$ (n times) and gives, in fact, a weight-preserving isomorphism of codes.

Thus it will entail no loss of generality in the future to assume that $f_{\alpha_1} = f_{\alpha_2}$ if and only if $\mathrm{Ker}\, f_{\alpha_1} = \mathrm{Ker}\, f_{\alpha_2}$, and we will habitually do so.[9]

The important class of *cyclic* codes was introduced in 1957 by Prange. We give here a definition and a brief treatment in our terms to illustrate the present approach.

$A; f_\alpha$, $\alpha \in \mathfrak{A}$ is said to be cyclic provided there is a function $J: A \to A$ and an encoding function f such that J^n is the identity and fJ^i yield the encoding functions as i runs from 1 to n. (Notice that any encoding function would do as an f once we know one exists.)

Equivalently, A is cyclic if and only if there is a map of codes $J: A \to A$ such that $J^n = 1$ and the induced map of the index set is a permutation which is a cycle of length n.

Suppose that A is cyclic of block length n and J has order k; i.e., $J^k = 1$ but $J^{k'} \neq 1$ for $k' < k$. Then k divides n and A has k distinct encoding functions each repeated n/k times. To see this, we pick an f which is an encoding function. Clearly $fJ, \cdots, fJ^k$ exhausts the distinct encoding functions. Now if $f = fJ^r$ with $r < k$ then $g = gJ^r$ for every encoding function g. But this means (in virtue of the coding axiom) that $J^r = 1$, which is impossible. Thus $fJ, \cdots, fJ^k$ are the distinct encoding functions, and each is repeated n/k times.

[9] When K is a field, an automorphism of K as K-module is simply multiplication by some fixed nonzero field element. Thus our identification of functionals is, in this case, the usual identification in affine space which yields projective space of one less dimension. Gleason and MacWilliams have successfully applied projective methods to error-correcting codes.

It follows in particular that cyclic codes of prime block length never have "repeated columns."

For a cyclic linear code J is, of course, a homomorphism, hence an automorphism, of A. In this case, if f is any of the encoding functions of A, then kernel f does not contain any proper invariant subspace of J (since $0 = \bigcap \ker f_\alpha = \bigcap J^i(\ker f)$). Conversely, if K is a ring, A a K-module, f a homomorphism from A to K, and J an automorphism of A of order dividing n such that no proper invariant subspace of J is contained in kernel f, then fJ^i, $i = 0, 1, \cdots, n-1$, are encoding functions for a cyclic code of block length n.

We now sketch the classical theory in our language. Thus let K be a finite field of q elements, and let A be a cyclic code of linear dimension k over K. In the light of the remark above concerning repetitions for cyclic codes, we assume the block length of A to be the order n of J. Then we can prove:

(i) As a code, A has dimension $k \leqq n$ (as remarked in Section I).

(ii) A is recursive[10] for the minimal polynomial $m(x)$ of J, and $m(x) \mid (x^n - 1)$.

(iii) If we realize the code as n-tuples $(a_0, \cdots, a_{n-1})$ over K, where each $a_i = f_i(a)$, $a \in A$, then an n-tuple $(b_0, \cdots, b_{n-1})$ over K belongs to the code if and only if the polynomial $b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1}$ (in $K[x]$) is a multiple of $(x^n - 1)/m(x)$.

Since in general any set of functionals spans the dual space A^* of A if and only if the intersection of their kernels is 0, we know that the encoding functions $f_0, \cdots, f_{n-1}$ span A^*; thus as a code, A has dimension k, which proves (i). Since A^* has dimension k, $f_0, \cdots, f_k$ are linearly dependent, from which it follows on applying J repeatedly that $f_0, \cdots, f_{k-1}$ span $f_0, \cdots, f_{n-1}$.

It follows that in the linear dependence

$$c_0f_0 + \cdots + c_kf_k = 0, \qquad c_i \in K, \tag{2}$$

we must have $c_k \neq 0$. Then the polynomial $c_0 + c_1 x + \cdots + c_kx^k = m(x)$ has degree k and satisfies $f_im(J) = 0$ for all i. Thus $m(J)\, A \subset \bigcap \ker f_i = 0$, or $m(J) = 0$. Since any polynomial relation for J yields an equation of the form (2), J satisfies no polynomial of degree less than k.

The code is now recursive for $m(x)$, as multiplication of (2) by J^i,

[10] This means that if $m(x) = c_0x^r + c_1x^{r-1} + \cdots + c_r$, then the realization of A consists of all n-tuples $(a_0, a_1, \cdots, a_{n-1})$ over K such that $c_0a_{i+r} + c_1a_{i+r-1} + \cdots + c_ra_i = 0$, $i = 0, 1, \cdots, n-r-1$.

$0 \leqq i \leqq n - k - 1$, immediately shows. Every vector satisfying this recursion belongs to the code, since $f_0, \cdots, f_{k-1}$ are linearly independent. Thus we have proved (ii).

Now $m(x)$ divides $(x^n - 1)$, since it is the minimal polynomial of J.

We omit the quite standard proof of (iii).

One can easily show that a code which is cyclic in the usual sense is cyclic in our sense. Therefore a code over a finite field is cyclic in the classical sense if and only if it is cyclic in our sense.

Our last statement on cyclic codes is an apparently new lower bound on the minimum weight.

THEOREM. *Let A be a cyclic (n, k) code over the finite field K, with automorphism J. Then the minimum weight d of A satisfies*

$$d \geqq n/k.$$

If J has order k, then $d = n/k$. Conversely, if $d = n/k$ and if $(d, q - 1) = 1$, then J has order k.

PROOF: We realize the code as a space of n-tuples $(a_0, \cdots, a_{n-1}) = (f_0(a), \cdots, f_{n-1}(a))$, $a \in A$, where the f_i are the encoding functions. We first remark that $a \neq 0$ implies that $(a_{i+1}, \cdots, a_{i+k}) \neq (0, \cdots, 0)$ for each i.

Now consider the case $k \mid n$. Here we must immediately have $d \geqq n/k$, in view of the above remark. If J has order k, then $d = n/k$ trivially, so we turn to the converse. Let $d = n/k$, and let $w(a) = d$; then there is exactly one nonzero a_i in each block of k consecutive coordinates. After cycling we may assume $a_0 \neq 0$. It follows that $a_k \neq 0$, $a_{2k} \neq 0$, $\cdots$, $a_{(d-1)k} \neq 0$, and that all other $a_i = 0$. Let us assume $a_0 = 1$. Then $a - a_k^{-1} J^k(a)$ has its first k coordinates all 0 and is therefore 0. Thus $J^k(a) = a_k \cdot a$, or (putting $a_k = c$) $(a_0, a_k, \cdots, a_{(d-1)k}) = (1, c, c^2, \cdots, c^{d-1})$, implying that we must have $c^d = 1$. Thus if $(d, q - 1) = 1$, then $c = 1$, implying $J^k(a) = a$. The k vectors $a, Ja, \cdots, J^{k-1}a$ are easily seen to form a basis for the code. Hence, $J^k = 1$. (The example with $n = 4$, $k = 2$ given by $\{c(1, 0, -1, 0) + c'(0, -1, 0, 1); c, c' \in K = GF(3)\}$, is a cyclic code with $d = n/k = q - 1 = 2$ for which J has order n not k. Thus the assumption $(d, q - 1) = 1$ is needed.)

In case $k \nmid n$, let $n = tk + r$, $0 < r < k$. We then obviously have $d \geqq t$, so let us assume $d = t = w(a)$ and find a contradiction. Let $a = (a_0, \cdots, a_{n-1})$ with the nonzero a_i given by $a_{i_1}, \cdots, a_{i_t}$, where $i_1 < i_2 < \cdots < i_t$. Then we must have $i_2 - i_1 \leqq k$, $i_3 - i_2 \leqq$

$k, \cdots, i_t - i_{t-1} \leqq k$ and also $n + i_1 - i_t \leqq k$. If we add these t inequalities together, we find $n \leqq tk$, a contradiction. Thus $d \geqq t + 1 \geqq n/k$.

In the classical case $q = 2$, the assumption $(q - 1, d) = 1$ is automatically satisfied, and our theorem becomes: For a cyclic (n, k) code over $\{0, 1\}$ the minimum weight d satisfies $d \geqq n/k$, with equality if and only if the code consists of all vectors of the form

$$(a_0, a_1, \cdots, a_{k-1}; a_0, a_1, \cdots, a_{k-1}; \cdots; a_0, \cdots, a_{k-1}).$$

That is, in the latter case, every code-vector is the d-fold repetition of its first k coordinates; and every such vector is in the code.

The result says that in order to correct errors by means of cyclic codes, the least effective scheme is repetition. It partly justifies the intuitive feelings of Slepian (1960, p. 1251) and MacWilliams (1961, p. 296) against repeated columns. Interestingly enough, repetition was the earliest approach to error-correction (Wozencraft and Reiffen, 1961, p. 3).

In the next section we shall need the result that linear codes over a field are systematic. We include the proof as a second illustration of our approach. The coding axiom implies that the encoding functions span the dual of the code A. We can therefore choose k encoding functions $f_1, \cdots, f_k$ as a basis of the dual. Thus for each encoding function f_α of A there is a relation

$$f_\alpha = \sum_{i=1}^{k} c_{\alpha i} f_i, \qquad c_{\alpha i} \in K;$$

and this is what it means to say a code is systematic.

III. THE MAPPING THEOREM

We continue to make the three assumptions at the beginning of Section II. We shall also make the following assumptions:

1°. Each encoding function maps A onto K.

2°. The number of elements of A is q^k, where k is dim A.

3°. Two encoding functions are equal if and only if their kernels are equal.

4°. If f and g are distinct encoding functions, then $\ker f \cap \ker g$ consists of q^{k-2} elements.

Except for 3°, these assumptions hold automatically when K is a field, so long as the zero function is not an encoding function. As for 3° there is no loss of generality in making that assumption even when K

is a ring; when K is a field, note again that we are simply identifying the linear functional f with αf, $\alpha \neq 0$, $\alpha \in K$, when we make assumption 3°. Assumption 2° is the statement that A is an (n, k) code as defined in Section I.

The assumption in 4° does not necessarily hold when K is not a field. For example, let $K = Z_4$ (the ring of integers modulo 4) and let $A = Z_4 \oplus Z_4$. Define three K-homomorphisms by

$$f_1(x, y) = x + y,$$

$$f_2(x, y) = y,$$

$$f_3(x, y) = 2x + y,$$

Then $\bigcap_{\alpha=1}^{3} \ker f_\alpha = 0$, since already the common kernel of f_1 and f_2 is $(0, 0)$. Thus A, f_1, f_2, f_3 form a code of dimension $k = 2$ over K. Assumptions 1° and 2° hold, but 4° does not, since $\ker f_2 \cap \ker f_3 = \{(0, 0), (2, 0)\}$ consists of 2 elements, not of $1 = q^{k-2}$ element.

The remainder of this section will be devoted to proving our main theorem and deriving some of its consequences. The reader familiar with the theory of group characters will recognize the method of proof (integration over the code).

MAPPING THEOREM. *Let A and B be two linear codes over K satisfying 1° through 4° and $\phi: A \to B$ be a map of codes. Then, denoting by w the Hamming weight function defined in Section II, we have*

$$\sum_{a \in A} w(a) w(\phi(a)) = (q - 1) q^{k-2} [mn(q - 1) + \sum_{\beta \in \mathfrak{B}} n_\beta],$$

where m is the block length of A, n the block length of B, and n_β the number of encoding functions of A equal to $g_\beta \phi$, g_β being the βth encoding function of B.

PROOF: Recall that $\chi: K \to Z$ is defined by $\chi(0) = 0$, $\chi(c) = 1$ for $c \neq 0$ and that χ_α and η_β denote, respectively, the maps χf_α and χg_β. As before we have

$$w(a) = \sum_{\alpha \in \mathfrak{A}} \chi_\alpha(a), \qquad w(b) = \sum_{\beta \in \mathfrak{B}} \eta_\beta(b), \qquad a \in A, b \in B. \quad (3)$$

Multiplying the first equality of (3) by $\eta_\beta(\phi(a))$ and summing over $\mathfrak{B}$ we obtain

$$w(a) w(\phi(a)) = \sum_{\alpha \in \mathfrak{A}} \sum_{\beta \in \mathfrak{B}} \eta_\beta(\phi(a)) \chi_\alpha(a). \quad (4)$$

Since ϕ is a map of codes, for each $\beta \in \mathfrak{B}$ we have $\eta_\beta \phi = \chi_{\alpha'}$ for some $\alpha' \in \mathfrak{A}$; and the number of such α' is precisely n_β.

The assumptions 1°–4° imply that

$$\sum_{a \in A} \chi_\alpha(a)\chi_{\alpha'}(a) = \begin{cases} (q-1)q^{k-1}, & \chi_\alpha = \chi_{\alpha'}, \\ (q-1)^2 q^{k-2}, & \chi_\alpha \neq \chi_{\alpha'}. \end{cases}$$

If we fix α' and sum this quantity over α, we obtain

$$\sum_{\alpha \in \mathfrak{A}} \sum_{a \in A} \chi_\alpha(a)\chi_{\alpha'}(a) = n'(q-1)q^{k-1} + (m-n')(q-1)^2 q^{k-2}, \quad (5)$$

where n' is the total number of α for which $\chi_\alpha = \chi_{\alpha'}$.

We now apply (5) to find the sum over A of (4). We have

$$\sum_{a \in A} w(a)w(\phi(a)) = \sum_{\beta} \Big(\sum_{\alpha} \sum_{a} \chi_\alpha(a)\chi_{\alpha'}(a) \Big),$$

where $\chi_{\alpha'} = \eta_\beta \phi$ as above. Thus from (5) we find

$$\sum_{a \in A} w(a)w(\phi(a)) = \sum_{\beta} [n_\beta (q-1)q^{k-1} + (m-n_\beta)(q-1)^2 q^{k-2}],$$

and since $\mathfrak{B}$ has n elements,

$$\sum_{a \in A} w(a)w(\phi(a)) = (q-1)q^{k-2}[mn(q-1) + \sum_{\beta \in \mathfrak{B}} n_\beta].$$

REMARKS

1. The mapping theorem can easily be extended to the case when some encoding functions of A are 0. One finds, making assumptions 1° through 4° for the nonzero encoding functions, and letting $m = m_0 + m_1$, where m_0 is the number of f_α which are 0, m_1 the number which are not 0, and n' the number of $\beta \in \mathfrak{B}$ such that $g_\beta \phi$ is 0, that

$$\sum_{a \in A} w(a)w(\phi(a)) = (q-1)q^{k-2} \cdot [m_1(n-n')(q-1) - n'm_0 + \sum_{\beta \in \mathfrak{B}} n_\beta].$$

This version includes the theorem, which is the case with $n' = m_0 = 0$.

In either case we may have $n' = 0$. For example, if ϕ is onto and no g_β is 0, then $n' = 0$. Also, of course, if no f_α is 0, then n' is trivially 0.

2. A special case of the theorem which may be important in applications arises when A is given concretely as a subspace of ΠK and ϕ is the projection on certain of the coordinates (e.g., shortening the code).

That is, one chooses certain indices $1 \leqq i_1 < \cdots < i_n \leqq m$ and defines ϕ by setting $\phi(a) = (a_{i_1}, \cdots, a_{i_n})$ for each $a = (a_1, \cdots, a_m)$ in A.

The result we have just obtained is similar to the orthogonality relations for group characters.

COROLLARY 1. *Suppose that all the encoding functions of A are distinct. Then*

$$\sum_{a \in A} w(a)w(\phi(a)) = (q-1)q^{k-2}\, n[m(q-1)+1].$$

PROOF: Each n_β is 1.

COROLLARY 2. *For any code A we have*

$$\sum_{a \in A} w(a)^2 = (q-1)q^{k-2}\left[m^2(q-1) + \sum_{i=1}^{r} j_i^2\right],$$

where m is the block length and r is the number of distinct encoding functions $f_1, \cdots, f_r$ of A, each f_i appearing exactly j_i times.

PROOF: Take $A = B$, and ϕ the identity map. (A generalization of this corollary has been proved by Pless (1963). Zierler (1962) has given an independent proof of it for the classical case.)

Remark. This result, though easy to derive, seems to have gone unnoticed even for the classical case $K = GF(2)$. There, it says that the sum of the squares of the weights of an (n, k) code with "no repeated columns" is $n(n+1)2^{k-2}$. This result allows us to find the weight-distribution for certain cyclic codes (Assmus-Mattson, 1961).

Many authors have interested themselves in bounds, for given m and k, on the minimum weight for linear codes. The next corollary gives such a bound and establishes economically conditions under which there exist codes optimal with respect to this bound. It is interesting that codes having all nonzero vectors with the same weight were among the first studied.

COROLLARY 3. *With the notation of Corollary 2, let s denote the minimum of the multiplicities $j_1, \cdots, j_r$. Then*

$$d \leqq \frac{m(q-1)+s}{q}. \tag{6}$$

Moreover, the following conditions (i), (ii), *and* (iii) *are mutually equivalent*:

(i) *All nonzero vectors of A have the same weight.*

(ii) $m = s(q^k - 1)/(q-1)$ and $d = sq^{k-1}$.

(iii) $m/d = (q^k - 1)/(q-1)q^{(k-1)}$.

Furthermore, any of (i), (ii), *or* (iii) *implies the following conditions* (iv) *and* (v) *in general; and when K is a field,* (v) *implies* (i), (ii), *and* (iii):

(iv) $d = (m(q-1)+s)/q$, *i.e., equality holds in* (6).

(v) $j_1 = j_2 = \cdots = j_r\ (=s)$ *and* $r = (q^k-1)/(q-1)$.

PROOF: Let f be an encoding function of A which is repeated exactly s times. Let B be the code it defines via the quotient process described in Section I and $\phi: A \to B$ the natural map. Apply the Mapping Theorem to obtain

$$\sum_{\substack{a\in A \\ f(a)\neq 0}} w(a) = (q-1)q^{k-2}(m(q-1)+s).$$

Now since $d \leqq w(a)$ for all nonzero $s \in A$ we have

$$(q-1)q^{k-1}d \leqq (q-1)q^{k-2}(m(q-1)+s),$$

with equality if all nonzero $a \in A$ have weight d. This yields the inequality (6). It also shows that (i) implies (iv).

The equivalence of (i) and (iii) was proved in the Proposition of Section II.

To prove that (i) implies (ii),[11] we use what we have just proved, namely,

$$d = \frac{m(q-1)+s}{q},$$

and (iii), which yields

$$d = \frac{(q-1)mq^{k-1}}{q^k-1}.$$

If we combine both these equations, we get (ii). Conversely, if (ii) holds, then (iii) follows immediately. Thus (i), (ii), and (iii) are mutually equivalent.

To prove that (i) implies (v), we apply the Mapping Theorem as above to the case of an arbitrary encoding function f_i of A. We find:

$$\sum_{\substack{a\in A \\ f_i(a)\neq 0}} w(a) = (q-1)q^{k-2}(m(q-1)+j_i).$$

The number of summands on the left-hand side here is $q^k - q^{k-1}$, since

[11] We are grateful to W. Wesley Peterson for correcting an earlier "proof" of this result.

f_i is onto. If now all nonzero vectors have the same weight, the left-hand side is $(q^k - q^{k-1})d$ for each i; thus $j_1 = \cdots = j_r$. Since $m = \sum j_i = rs$, the rest follows from (ii).

To prove the converse when K is a field, we simply note that $(q^k - 1)/(q - 1)$ is the number of encoding functions distinct in our sense. Thus when we use them all, each nonzero $a \in A$ annihilates $(q^{k-1} - 1)/(q - 1)$ of them, giving

$$w(a) = \frac{q^k - 1}{q - 1} - \frac{q^{k-1} - 1}{q - 1} = q^{k-1}. \qquad \text{Q.E.D.}$$

REMARKS

0. The code over $GF(2)$ having (10011), (11100), and (01111) as its nonzero vectors shows that (iv) does not imply (i).

1. Questions similar to those of Corollary 3 are dealt with by MacWilliams (1961, Section V) and McCluskey (1959, Section VI).

2. When K is a field, it is well known that codes with $d = [m(q - 1) + 1]/q$ exist. In this case $m = (q^k - 1)/(q - 1)$ is the number of linear functionals on k-dimensional space distinct in our sense. These codes are the so-called maximal-length shift-register sequences noted by Singer (1938) (also see (Zierler, 1959, p. 40)) and also are among the earliest Bose and Ray-Chaudhuri (1960) codes, which are also discussed in Peterson (1961, Chapter 9).

3. Corollary 3 can be used to answer a question arising out of Mattson-Solomon (1961). Suppose $m = 2h + 1$ (again $q = 2$) and let the minimum weight be $h + 1$ for an (m, h) code. Then since $h + 1 = (m + 1)/2$, all vectors in the code have the same weight; thus $m = 2^h - 1$, from the Corollary. This implies that $h = 3$ and $m = 7$. Thus the only code of the type considered in (Mattson-Solomon, 1961, Section 3)—namely, those for which $p = m = 2h + 1$ and 2 has multiplicative order h mod. p—which has minimum weight $h + 1$ is the (7, 3) cyclic code. Similarly, the only such code of minimum weight h is the (7, 4) cyclic code.

4. The above bound is frequently extremely poor. One gets immediately (since linear codes over fields are systematic) that when K is a field

$$d \leqq m - k + 1,$$

since all but one of the information places can be chosen to be zero and

one still gets a nonzero vector. In fact this inequality holds in a more general situation, namely, when K is a finite ring and the code is a not necessarily linear (n, k) code over K, provided we define d as the minimum distance between code-words. Joshi (1958, Thm. 1, p. 290) has proved this result for the classical case. His proof, being quite general, really shows that

$$N \leqq q^{n-d+1},$$

where N is the cardinality of the code. Joshi (1958, Thm. 2) proves a sharper result for linear codes in the classical case, namely, that $d \leqq n - k$ when $n > d > 2$. This bound, however, does not hold in general, as the next remark shows.

5. Let $K = GF(32)$, and let β be any primitive 11th root of unity. Then $\beta + \beta^{-1} = c$ is in K (since $c^{32} = \beta^{32} + \beta^{-32} = \beta^{-1} + \beta = c$) and β and β^{-1} are the roots of the polynomial $f(x) = x^2 + cx + 1 \in K[x]$. Therefore, the (11, 2) code A defined recursively by $f(x)$, namely, all vectors $a = (a_0, \cdots, a_{10})$ with $a_{i+2} = ca_{i+1} + a_i$, $i = 0, 1, \cdots, 8$, the a_i being chosen from K, is a cyclic code to which the method of Mattson-Solomon (1961, Section 2) applies. That is, if ζ is any 11th root of unity other than 1, then there is a polynomial $g_a(x) = c_0 + c_1 x^{e_1} + c_2 x^{e_2}$, where ζ^{e_1} and ζ^{e_2} are the roots of $f(x)$, such that $g_a(\zeta^i) = a_i$, $i = 0, 1, \cdots, 10$. Since $(x^{11} + 1)/f(x)$ is divisible by $x + 1$, the characterization of cyclic codes in Section II tells us that

$$c_0 = \sum_0^{10} a_i = 0.$$

If we now choose $\zeta = \beta^{-2}$ we find that $\zeta^5 = \beta$ and $\zeta^6 = \beta^{-1}$. Thus we may take $e_1 = 5$ and $e_2 = 6$, which gives $g_a(x)$ the form $x^5(c_1 + c_2 x)$ for each $a \in A$, which means that $g_a(x)$ has at most one zero on the group of 11th roots of unity, or in other words that $d \geqq 10 = n - k + 1$.

RECEIVED: August 31, 1962

REFERENCES

ASSMUS, JR., E. F. AND MATTSON, H. F. (1961), On determining the weight-distribution in cyclic codes of prime block length. Engineering Note 253, Applied Research Laboratory, Sylvania Electronic Systems, Waltham, Mass.

BOSE, R. C. AND RAY-CHAUDHURI, D. K. (1960), On a class of error correcting binary group codes. *Inform. and Control* **3**, 68–79 (Part I).

BOSE, R. C. AND KUEBLER, ROY R. (1960), A geometry of binary sequences asso-

ciated with group alphabets in information theory. *Ann. Math. Statist.* **31,** 113–139.

JOSHI, D. D. (1958), Upper bounds for minimum distance codes. *Inform. and Control* **1,** 289–295.

MACWILLIAMS, JESSIE (1961), Error-correcting codes for multiple-level transmission. *Bell System Tech. J.* **40,** 281–308.

MATTSON, H. F. AND SOLOMON, GUSTAVE (1961), A new treatment of Bose-Chaudhuri codes. *J. Soc. Indust. Appl. Math.* **9,** 654–669.

MCCLUSKEY, E. J., JR. (1959), Error-correcting codes—A linear programming approach. *Bell System Tech. J.* **38,** 1485–1512.

PETERSON, W. WESLEY (1961), "Error Correcting Codes." M.I.T. Press and Wiley, New York.

PLESS, VERA (1963), Power moment identities on weight distributions in error-correcting codes. *Inform. and Control* **6,** 147–152.

PRANGE, EUGENE (1957), Cyclic error-correcting codes in two symbols. AFCRC-TN-57-103, USAF Cambridge Research Laboratories, Bedford, Mass.

PRANGE, EUGENE (1961), Step-by-step decoding in groups with a weight function, (Part I). USAF Cambridge Research Laboratories Report 716, Bedford, Mass.

SINGER, JAMES (1938), A Theorem in finite projective geometry and some applications to number theory. *Trans. Am. Math. Soc.* **43,** 377–385.

SLEPIAN, DAVID (1956), A class of binary signaling alphabets. *Bell System Tech. J.* **35,** 203–234.

SLEPIAN, DAVID (1960), Some further theory of group codes. *Bell System Tech. J.* **39,** 1219–1252.

WEINITSCHKE, H. (1957), On some upper bounds of importance in Slepian's theory of coding. Tech. Memo. No. 15, Parke Math. Labs., Inc., Carlisle, Mass.

WOLFOWITZ, J. (1957), The coding of messages subject to chance errors. *Ill. J. Math.* **1,** 591–606; *ibid.* **2,** 137–141, 454–458; *ibid.* **3,** 477–489.

WOZENCRAFT, J. AND REIFFEN, B. "Sequential Decoding." Technology Press and Wiley, Cambridge, Mass., 1961.

ZIERLER, NEAL (1959), Linear recurring sequences. *J. Soc. Indust. Appl. Math.* **7,** 31–48.

ZIERLER, NEAL (1962), A note on the mean square weight for group codes. *Inform. and Control* **5,** 87–89.